

Qualys Web Application Scanning

Training Documents

- Download the Presentation Slides and Lab Tutorial Supplement from:
 - Qualys Sharepoint site - <https://bit.ly/qsc2021-was>

Lab Tutorial Supplement

- All lab activity for this course is performed in a simulated lab environment
- Please refer to the WAS Lab Tutorial Supplement for the following:
 - Link to start the lab (each lab topic has a separate link)
 - Overview of the steps performed for each topic
 - Additional supporting information

Additional Reading

- WAS Getting Started Guide - <https://www.qualys.com/docs/qualys-was-getting-started-guide.pdf>
- WAS API User Guide - <https://www.qualys.com/docs/qualys-was-api-user-guide.pdf>

Agenda

- ☐ WAS Overview
- ☐ Basic Web Application Setup and Discovery
- ☐ Advanced Web Application Setup and Scanning
- ☐ API Testing
- ☐ WAS Reporting
- ☐ Tagging and Users
- ☐ Burp and Bugcrowd Integration
- ☐ Malware Detection

Web Application Scanning Overview

WAS Overview

Automated Testing (Fault Injection)

- Submit “specially crafted” characters
- Observe the server’s response
- This represents 80 – 85% of Web app vulnerabilities

Manual Testing (BURP Integration)

- Automated tools effectively detect Web application bugs (SQL execution inside user input)
- Human beings are much better at discovering program design flaws

What Do Automated Tools Miss?

Logic Errors: Point of authentication vs. point of authorization

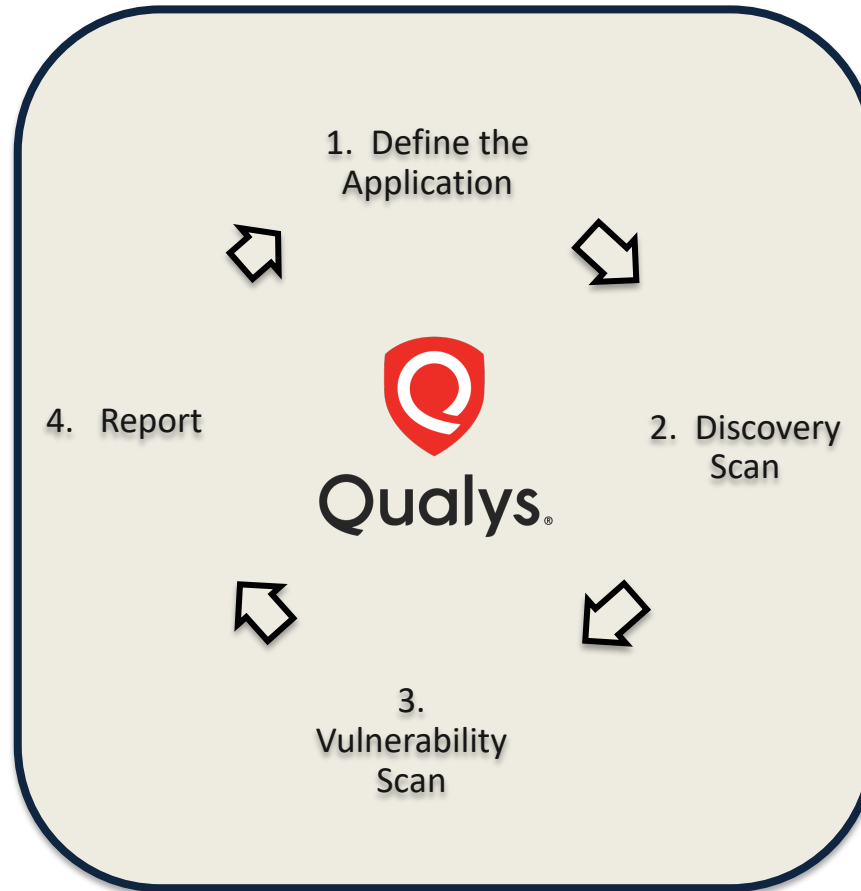
- Forced Browsing Links - user forces access to unauthorized link.

Permission Errors: File system permissions have a significant impact on application security.

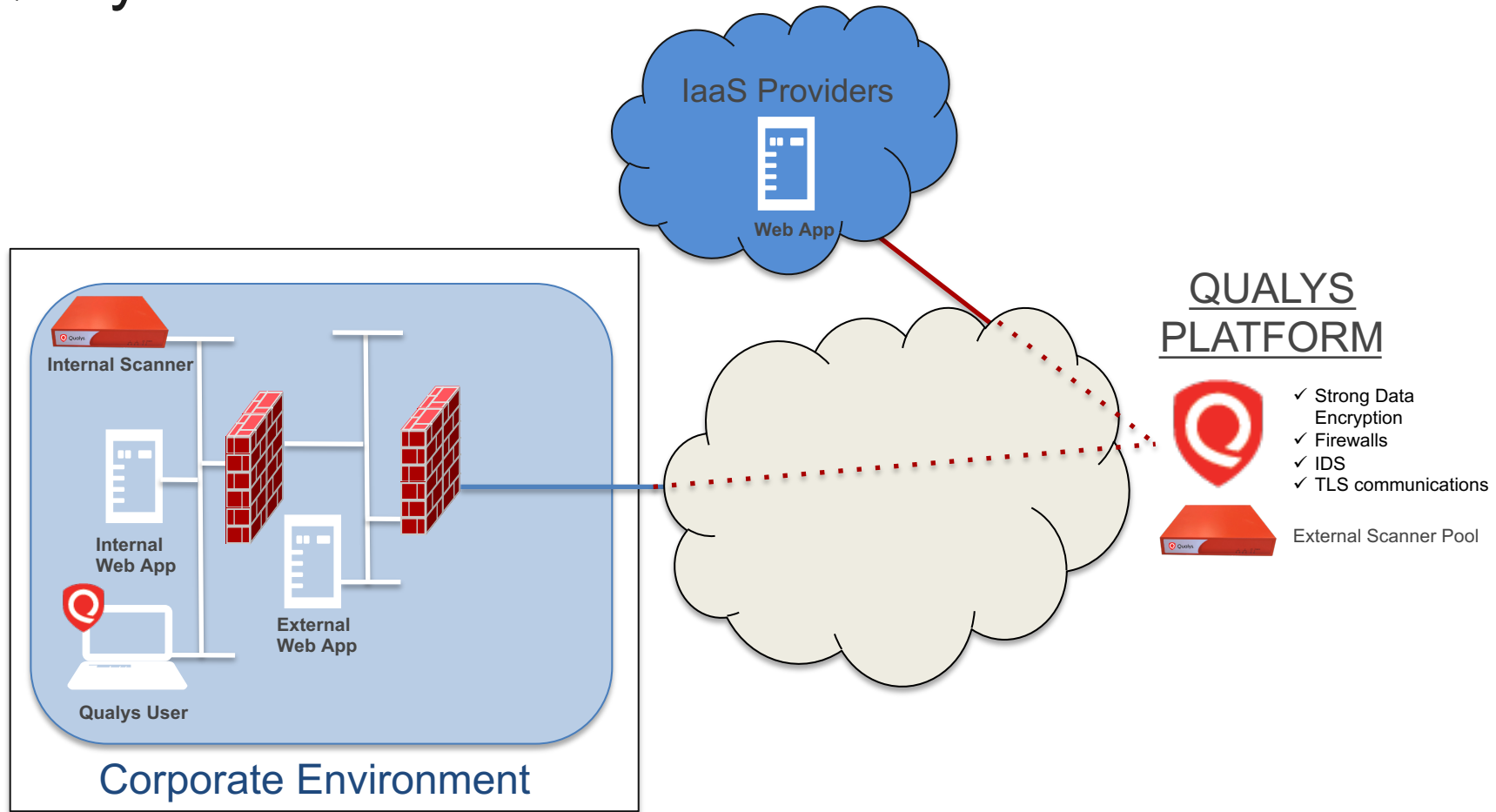
- Public file share that has employee payroll and medical records.

These typically require manual testing and detection.

Qualys WAS Lifecycle



Qualys Cloud Platform



KnowledgeBase and Search Lists

What do we check for?

Web Application Scanning

HelpShyam RajLog out

DashboardWeb ApplicationsScansDetectionsReportsConfigurationKnowledgeBase

KnowledgeBase

KnowledgeBase

Search Results

Search

Filter Results

Clear All

Identification

Clear

Category

Web Application










Vendor

Actions (0)

1 - 20 of 342

	QID	Name	Information	Category	Severity
<input type="checkbox"/>	150125	File Upload Form Found		Web Application	<div><div></div><div></div><div></div><div></div></div>
<input type="checkbox"/>	150252	Telerik Web UI Cryptographic Security Bypass Vulnerability	...	Web Application	<div><div></div><div></div><div></div><div></div></div>
<input type="checkbox"/>	150261	Subresource Integrity (SRI) Not Implemented		Web Application	<div><div></div><div></div><div></div><div></div></div>
<input type="checkbox"/>	150280	Wordpress Plugin Sitemap Stored XSS Vulnerability		Web Application	<div><div></div><div></div><div></div><div></div></div>
<input type="checkbox"/>	150287	Ruby on Rails File Content Disclosure Vulnerability	...	Web Application	<div><div></div><div></div><div></div><div></div></div>
<input type="checkbox"/>	150300	HTTP Request Smuggling		Web Application	<div><div></div><div></div><div></div><div></div></div>

Web App Vulnerabilities

Severity	Level	Description	Confirmed Vulnerabilities
	Minimal	Basic information disclosure (e.g. web server type, programming language) might enable intruders to discover other vulnerabilities, but lack of this information does not make the vulnerability harder to find.	
	Medium	Intruders may be able to collect sensitive information about the application platform, such as the precise version of software used. With this information, intruders can easily exploit known vulnerabilities specific to software versions. Other types of sensitive information might disclose a few lines of source code or hidden directories.	
Severity	Level	Description	Potential Vulnerabilities
	Minimal	Presence of this vulnerability is indicative of basic information disclosure (e.g. web server type, programming language) and might enable intruders to discover other vulnerabilities. For example in this scenario, information such as web server type, programming language, passwords or file path references can be disclosed.	
	Medium	Presence of this vulnerability is indicative of basic information disclosure (e.g. web server type, programming language) and might enable intruders to discover other vulnerabilities. For example version of software or session data can be disclosed, which could be used to exploit.	
Severity	Level	Description	Sensitive Content
	Minimal	Sensitive content was found in the web server response. During our scan of the site form(s) were found with field(s) for credit card number or social security number. This information disclosure could result in a confidentiality breach and could be a target for intruders. For this reason we recommend caution.	
	Medium	Sensitive content was found in the web server response. Specifically our service found a certain sensitive content pattern (defined in the option profile). This information disclosure could result in a confidentiality breach and could be a target for intruders. For this reason we recommend caution.	
Severity	Level	Description	Information Gathered
	Minimal	Intruders may be able to retrieve sensitive information related to the web application platform.	
	Medium	Intruders may be able to retrieve sensitive information related to internal functionality or business logic of the web application.	
	Serious	Intruders may be able to detect highly sensitive data, such as personally identifiable information (PII) about other users of the web application.	

Search Lists Overview

User-defined Groups of QIDs

- Static search list - Manually defined
- Dynamic search list - Criteria-based

Benefits

- Dynamic List updates when new QIDs meet the search criteria
- No limitation to the number of QIDs in search list

Search Lists Overview

Search lists allow you to modify the vulnerabilities for which you are:

- Scanning
- Reporting

Example:

- Run a scan for only SQLi
- Exclude a vulnerability from a scan
- Build a report for only XSS

The screenshot shows the 'Dynamic Search List Creation' window, specifically 'Step 2 of 4: Search Criteria'. The interface has a blue header bar with the title and a 'Turn help tips: On | Off Launch help' link. On the left, a vertical sidebar shows four steps: 1 List Details (checked), 2 Search Criteria (active), 3 Comments, and 4 Review And Confirm. The main area is titled 'Enter search criteria' and contains a list of checkboxes for various search filters. The 'Category' filter is selected and set to 'Web Application'. Other filters include 'Patch Available', 'CVE ID', 'Exploitability', 'Associated Malware', 'Vendor Reference', 'CVSS Base Score', 'CVSS Temporal Score', 'CVSS Access Vector', 'BugTraq ID', and 'Service Modified'. At the bottom, there are checkboxes for 'Confirmed Severity' (selected) and severity levels: 'Level 1', 'Level 2', 'Level 3', 'Level 4', and 'Level 5' (selected). At the bottom of the window, there are buttons for 'Cancel', 'Check All', 'Clear', 'Test', 'Previous', and 'Continue'.

Dynamic Search List Creation Turn help tips: On | Off Launch help

Step 2 of 4

1 List Details ✓
2 **Search Criteria** ✓
3 Comments
4 Review And Confirm

Enter search criteria

☒ Category Web Application
☐ Patch Available
☐ CVE ID
☐ Exploitability
☐ Associated Malware
☐ Vendor Reference
☐ CVSS Base Score
☐ CVSS Temporal Score
☐ CVSS Access Vector
☐ BugTraq ID
☐ Service Modified
☒ Confirmed Severity
☐ Level 1 ☐ Level 2 ☐ Level 3 ☐ Level 4 ☒ Level 5

Cancel Check All Clear Test Previous Continue

Lab 1 and 2

Please follow **pages 3 – 5** from the Lab Tutorial Supplement

Lab Supplement - <https://bit.ly/qsc2021-was>

Lab 1 – KnowledgeBase

Lab 2 – Search Lists

A stylized illustration of a laptop screen. The screen is white and displays the text "15 min." in a black, sans-serif font. The laptop's frame is a light gray color, and the screen is slightly tilted back.

15 min.

Basic Application Setup and Discovery

Defining an Application

An application is:

- A business function typically requiring login
- Running unique code

Defining Applications – Unique Business Process

Example site:

<http://site/admin/>

<http://site/hr/>

<http://site/finance/>

Scenario 1:

- Each directory is part of a single app if they are part of an Intranet Portal
- (1 app total)

Scenario 2:

- Authentication credentials are different for each, with different business functions
- (3 apps total)

Defining Applications – Different ports

Example site:

E-commerce site that authenticates over https, allows browsing over http a catalog:

`https://e-commerce:443/login.cgi`

`http://e-commerce:80/browse.cgi`

Scenario:

- WAS users only need to define the *starting* port.
- The scanner will discover all ports in other links.
- (1 app total)

Defining Applications – Different Ports

Example site:

<http://intranet:80/index.cgi>

<http://intranet:8080/index.cgi>

Scenario 1:

- If the app on port 80 has links to app on port 8080
- Links are same business function (1 app total)

Scenario 2:

- If app on port 80 doesn't have links to port 8080
- Links are different business functions
- (2 apps total)

Defining Applications – Different hostnames

Example site:

`http://production.domain:80/`

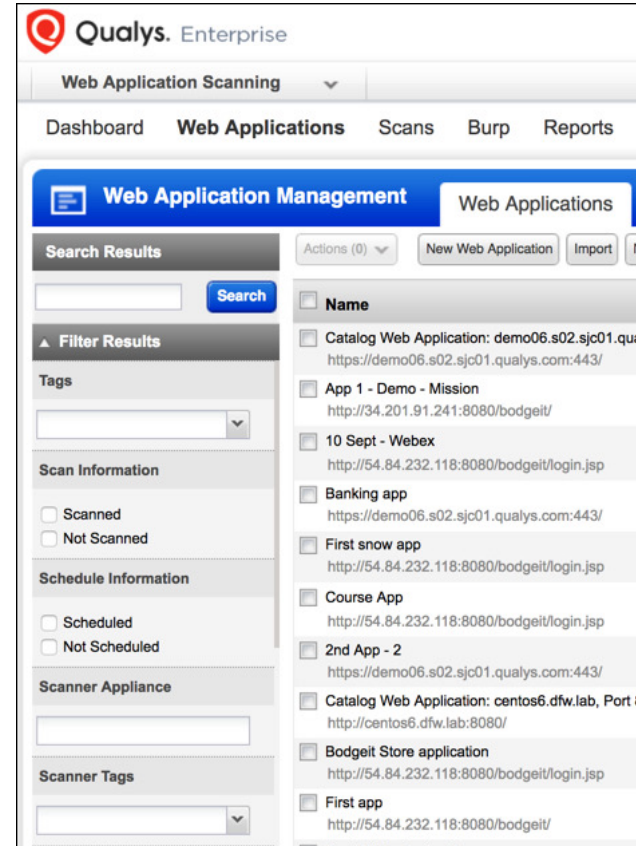
`http://qa.domain:80/`

Generally considered 2 applications
because they are separate
hostnames

Web Applications - Filtering

Filter your apps by:

- URL
- Tags
- Scan information
- Last Scan Date
- Last Scan Status
- Scanner Appliance
- Scanner Appliance Tags
- Authentication Record
- Custom Attribute
- Creation Date



Web Applications – Bulk Edit

Bulk Edit:

- Owner
- Scope
- Option Profile
- Scanner Appliance
- Header Injection
- Authentication Record

Web Application Edit: (3) Web Applications

Turn help tips: On | Off Launch help

Edit Mode

Asset Details

Application Details

Scan Settings

Authentication

Comments

Tell us the scan settings you'd like to change

3 web applications will be updated with your changes

Select the scan settings you want to edit. Once you click Save we'll apply the changes to all 3 web applications.

Default Scan Options

Choose the default scan settings for the web applications you've selected. You can change the defaults for each scan.

☒ Option Profile

Auth Option Profile

List last updated today 07:42am

View | Create

☐ Scanner Appliance

External

Individual

Tags (Set group)

☐ Lock this scanner appliance for this web application.

☐ Cancel Option

Do not Cancel Scan

Crawling Hints

Select these options and we'll crawl all links and directories found in these configuration files. This is a good way to be sure that the URLs in your sites are scanned.

Crawl all links and directories found in:

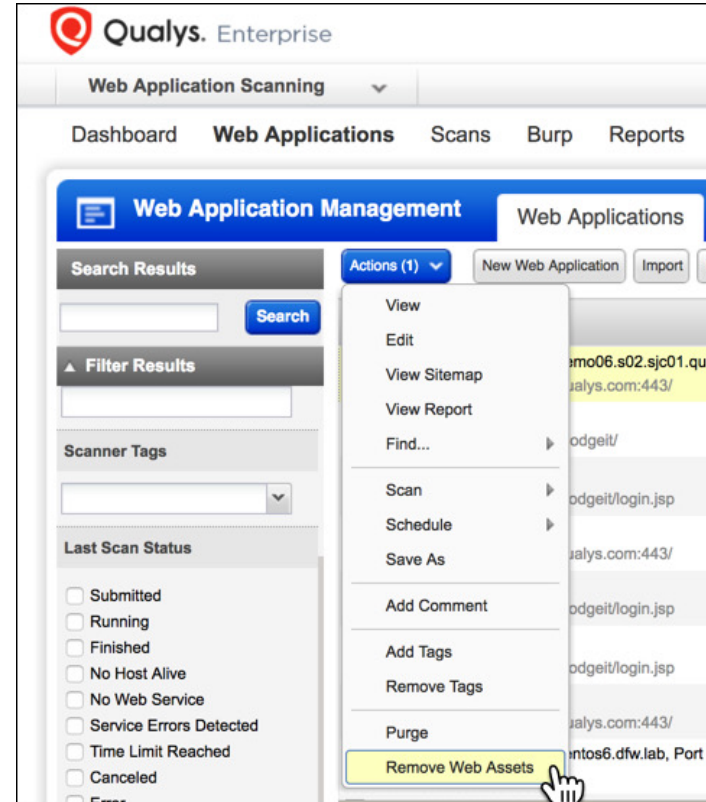
Cancel

Save

Removing Web Applications

Used to remove retired Applications

Like VM, does a full purge for that web app within Qualys



Crawl Scope

Crawl Scope

Web Application Edit: My First App

Edit Mode

Asset Details

Application Details

Scan Settings

Crawl Settings

Redundant Links

Tell us about the web application you want to scan

Target Definition

Web Application URL (or Swagger file URL)
https://demo06.s02.sjc01.qualys.com/

Crawl Scope*

Limit to content located at or below URL subdirectory

Limit at or below URL hostname (demo06.s02.sjc01.qualys.com)

Limit to content located at or below URL subdirectory

Limit to URL hostname and specified sub-domain

Limit to URL hostname and specified domains

Scope – Limit to URL hostname

Select this to crawl the hostname within the URL using http or https and any port

Example: `http://www.example.org/new`

- All links in the `http://www.example.org` domain will be crawled

`http://www.example.org/support`

`http://www.example.org:8080/news`

- Links from `www.example.org` will not be followed

`http://video.www.example.org`

`http://cdn.example.org`

Scope – Limit to content located at or below Sub-directories

We can limit crawling to the starting URI and its sub-directories.

Sample Web Application:

Virtual Host: `www.qualys.com`

Port: 80

Starting URI: `/research/`



Using the above web application, the scanning engine will start its scan at `http://www.qualys.com/research/`. From this page, links will be found to:

`http://www.qualys.com/research/exploits/`
`http://www.qualys.com/research/top10/`
`http://www.qualys.com/research/vulnlaws/`
`http://www.qualys.com/research/knowledge/`
`http://www.qualys.com/`
`http://www.qualys.com/products/qg_suite/`
`http://www.qualys.com/customers/`
etc...

From this list of links discovered, the scanning engine will NOT crawl:

`http://www.qualys.com/`
`http://www.qualys.com/products/qg_suite/`
`http://www.qualys.com/customers/`

Notes:

`http://www.qualys.com/` will not be crawled because it is a parent directory of `/research/`.

`http://www.qualys.com/products/qg_suite/` and `http://www.qualys.com/customers/` will not be crawled because they are not child directories of `/research/`.

Scope – Limit to URL hostname and specified sub-domain

We can limit it to crawl only sub-domains

Web Application URL

`https://demo06.s02.sjc01.qualys.com:443/`

Crawl Scope*

Limit to URL hostname and specified sub-domain

Restricted to sub-domain*

`.s02.sjc01.qualys.com`

Scope will be limited to URL `https://demo06.s02.sjc01.qualys.com/` and sub-domain `.s02.sjc01.qualys.com`, using HTTP or HTTPS and any port. All links discovered in `demo06.s02.sjc01.qualys.com` and in `.s02.sjc01.qualys.com` or any of its subdomains will be in scope. For example, links like these will be in scope: `https://demo06.s02.sjc01.qualys.com/support/`, `https://demo06.s02.sjc01.qualys.com:8080/logout/`, `https://s02.sjc01.qualys.com/images/` and `https://videos.s02.sjc01.qualys.com`. Any link whose domain does not match the web application URL hostname or is not a subdomain of `.s02.sjc01.qualys.com` will not be in scope. This means, for example, `https://videos.qualys.com` will not be included.

Scope – Limit to URL hostname and specified domains

We can crawl the starting URL, and the additional domains

Target Definition (*) REQUIRED FIELDS

Web Application URL
https://demo06.s02.sjc01.qualys.com:443/

Crawl Scope*
Limit to URL hostname and specified domains

Domains*
demo7.s02.sjc01.qualys.com

Scope will be limited to the URL hostname **https://demo06.s02.sjc01.qualys.com/**, domains **demo7.s02.sjc01.qualys.com** and any other, using HTTP or HTTPS and any port. All links discovered in **demo06.s02.sjc01.qualys.com**, **demo7.s02.sjc01.qualys.com** and all other domains specified will be in scope. This means, for example, these links will be included: **https://demo06.s02.sjc01.qualys.com/support/**, **https://demo06.s02.sjc01.qualys.com:8080/logout/** and **https://demo7.s02.sjc01.qualys.com/images/**. Links whose domain does not match web application URL hostname or one of the domains specified will not be in scope. For example, **https://videos.qualys.com** and **https://cdn.demo7.s02.sjc01.qualys.com** will not be included.

Scanning

Scan Types

Discovery Scan

- All links are determined
- Authentication is maintained during the scan
- Links with forms are set aside for vulnerability assessment

Vulnerability Scan

- Should happen after at least one Discovery Scan
- Tests the web application for vulnerabilities

Discovery Scan

Discovery

1. Scan begins at starting URL identified in the application definition
2. Using the Scope Options identified in the application definition, the scan traverses links to discover pages and content
3. Configuration data is collected from the target app and its host
4. Vulnerability testing is not performed

QID 150009 - Links Crawled

QID 150009
Links Crawled
lists all links
that have been
crawled

Information Gathered Details

150009 Links Crawled

Finding #	963436* (229777221)	Web Application	2nd App
Group	Information Gathered	Authentication	Not Used
CWE	-		
OWASP	-	Detection Date	13 Feb 2017 12:05PM GMT
WASC	-		

Details Show

Results

☒ Highlight changes from previous scan

- New - this link was not found in the previous scan
- Modified - this result was found by the previous scan but its value was different
- Removed - this link was not found, but was reported in the previous scan

Duration of crawl phase (seconds): 566.00
Number of links: 32
(This number excludes form requests and links re-requested during authentication.)

<https://demo06.s02.sjc01.qualys.com/>
<https://demo06.s02.sjc01.qualys.com/?account=business>
<https://demo06.s02.sjc01.qualys.com/?account=checking&ID=1>
<https://demo06.s02.sjc01.qualys.com/?account=credit&ID=1>
<https://demo06.s02.sjc01.qualys.com/?account=personal>
<https://demo06.s02.sjc01.qualys.com/?account=profiles&ID=1>
<https://demo06.s02.sjc01.qualys.com/?account=savings&ID=1>
<https://demo06.s02.sjc01.qualys.com/bog/>
<https://demo06.s02.sjc01.qualys.com/bog/aboutus.html>

Export...

Web Application Sitemap

View Web Application or Scan Sitemap To:

- View Pages Crawled and Vulnerability Statistics
- Create New Web Apps
- Add URLs to Black List
- Add URLs to White List

Web Application Sitemap: Catalog Web Application: demo06.s02.sjc01.qualys.com, Port 443

Use the filters below to alter list view for this application sitemap.

Page view filters: **C** Crawled 28 **R** Rejected 1 **E** External 2 **V** Vulnerabilities 44 **S** Sensitive Contents 0

Link in view: demo06.s02.sjc01.qualys.com:443

Actions (1) Export Sitemap 1 - 8 of 8

Link	Link Info.	Children Info.
..		
admin		
boq	1	26
Icons		1
includes		
phpMyAdmin		
?account=business	C	
?account=personal	C	3

Quick Actions

- Create Web Application
- Add To Black List
- Add To White List

Folder Information

Folder: https://demo06.s02.sjc01.qualys.com:443/boq/
Status: Crawled
Vulnerabilities: 1
Sensitive Content: 0

Children Information

Pages Crawled: 24
Vulnerabilities: 26

Assessment Details

Total Vulnerabilities: 26

- 2 Level 5
- 0 Level 4
- 9 Level 3
- 6 Level 2
- 9 Level 1

Crawling Details

Lab 3, 4 and 5

Please follow **pages 5 – 14** from the Lab Tutorial Supplement

Lab Supplement - <https://bit.ly/qsc2021-was>

Lab 3 – Create Application 1

Lab 4 – Create Application 2

Lab 5 – Scheduled Scans



20 min.

Advanced Application Setup and Scanning

Option Profile - Crawling

Crawl stops when:

- Max number of links threshold is met

Maximum crawl requests (the total number of links and forms to follow)*

8000

- No new links are discovered
- Scan time-out is reached

Cancel scan after



after

2



hours

Option Profile – Scan Parameters

- Modify Form submission for GET, POST, GET&POST, None
- Change User agent
- Create Parameter sets
- Ignore common binary files
- SmartScan Support
- Change Behavior and Performance settings
- Modify Bruteforcing settings

Please define how the scan will perform

General Settings (*) REQUIRED FIELDS

Form Submission* Post & Get

Form Crawl Scope ☐ Include form action URI in form uniqueness calculation.
When enabled, we'll calculate form uniqueness using form action URI in addition to form field names. This results in crawling of all forms having same fields but having different action URI.

Maximum links to test in scope* 300
Total number of links and forms to follow and test within the scan scope. If performing a Discovery Scan, this is the maximum links that will be crawled, as there will not be any testing performed

User Agent Example: Mozilla/4.04 (X11; I; SunOS 5.4 sun4m)

Request Parameter Set* Initial Parameters [View](#) [Create](#)

Document Type ☒ Ignore common binary files based on [file extensions](#).

SmartScan Support

When enabled we'll perform advanced scanning, using enhanced AJAX/SPA deep crawling and vulnerability testing, for a number of actions per page. This option is recommended for scanning sites with advanced frameworks and technologies.

☐ Enable SmartScan Support

Behavior Settings

These settings define the threshold to be reached before stopping the scan. If you deactivate these settings, the scan will keep running no matter how many errors it will find.

☒ Timeout Error Threshold 100

☒ Unexpected Error Threshold 300

Performance Settings

Scan Intensity* Low

Processes to run in parallel
Total processes: 10
HTTP processes: 2
HTTP request delay
Request delay: High

Bruteforcing Settings

☒ Use password bruteforcing

☐ User list

☒ System list Minimal

Option Profile – Enhanced Crawling

Crawling Options

☒ Enhanced Crawling

When enabled we will attempt to load and render individual directories. If unique content is found, we'll begin crawling from there to improve scan coverage.

- Improves scan coverage by re-crawling individual directories present in the links found during crawling
- Uses a directory chopping approach

Option Profile – Enhanced Crawling

- Starting URL – <https://www.example.com/foo/abc/xyz/register.php>
- First request – <https://www.example.com/foo/abc/xyz>
- Then crawl – <https://www.example.com/foo/abc>
- Then crawl – <https://www.example.com/foo>

Option Profile - SmartScan

- Used for enhanced AJAX or Single Page Applications (SPA)
- Supports sites using AngularJS and bootstrap
- View QID 150148 to see links crawled – this will be your hint to verify SmartScan is working

SmartScan Support

When enabled we'll perform advanced scanning, using enhanced AJAX/SPA deep crawling and vulnerability testing, for a number of actions per page. This option is recommended for scanning sites with advanced frameworks and technologies.

☒ Enable SmartScan Support

You can customize the number of actions that can be tested per page. Note the higher the number you set, the longer the scan duration.

SmartScan Depth*

Option Profile – Behavior Settings

Timeout Error: Network connectivity or someone reboots a server

Unexpected Error: Web app returning 500/Internal Server Errors

If a threshold is met, your scan will give you a “Service Errors Detected” status

Behavior Settings

These settings define the threshold to be reached before stopping the scan. If you deactivate these settings, the scan will keep running no matter how many errors it will find.

<input checked="" type="checkbox"/> Timeout Error Threshold	<input type="text" value="100"/>
<input checked="" type="checkbox"/> Unexpected Error Threshold	<input type="text" value="300"/>

Option Profile – Keyword URL Search

- Search for URL links that contain specific keywords
- Keywords are searched in internal links during Discovery/Vulnerability scan
- Links containing the specified keyword are shown under QID 150141

Keyword URL Search

☒ Keyword Search

customer

Specify strings or [regular expressions](#) to search for keywords in URLs. You may enter up to 10 keywords. Each keyword must be a minimum of 5 characters or a maximum of 200. Enter each keyword on a new line.

Option Profile – Bruteforcing

- Performed when Form Authentication is used
- Make sure you include QID 150049
- Use Qualys list or import your own

Bruteforcing Settings

☒ Use password bruteforcing

☐ User list

☒ System list

Web Application - Explicit URLs to Crawl

- Specify URLs you want the service to crawl
- Useful for pages not linked to other pages in the application

Edit Mode

- Asset Details
- Application Details**
- Scan Settings
- Crawl Settings
- Redundant Links
- Authentication
- Crawl Exclusion Lists
- Advanced Options
- Malware Monitoring
- Comments
- Action Log

Tell us about the web application you want to scan

Target Definition (*) REQUIRED FIELDS

Web Application URL
https://demo06.s02.sjc01.qualys.com:443/

Crawl Scope*

Limit at or below URL hostname (demo06.s02.sjc01.qualys.com)

Scope will be limited to the hostname within the URL: https://demo06.s02.sjc01.qualys.com/, using HTTP or HTTPS and any port. All links discovered on the demo06.s02.sjc01.qualys.com domain will be in scope. For example, all links discovered in https://demo06.s02.sjc01.qualys.com/support/ and https://demo06.s02.sjc01.qualys.com:8080/logout/ will be in scope. Links outside the demo06.s02.sjc01.qualys.com domain are not in scope. This means, for example, links like https://demo06.s02.sjc012.qualys.com and https://cdn.demo06.s02.sjc01.qualys.com will not be in scope.

Explicit URLs to Crawl / REST Paths and Parameters / SOAP WSDL Location

https://demo06.s02.sjc01.qualys.com/aade3aEfjafae.htm
https://demo06.s02.sjc01.qualys.com/webservices/wSDL

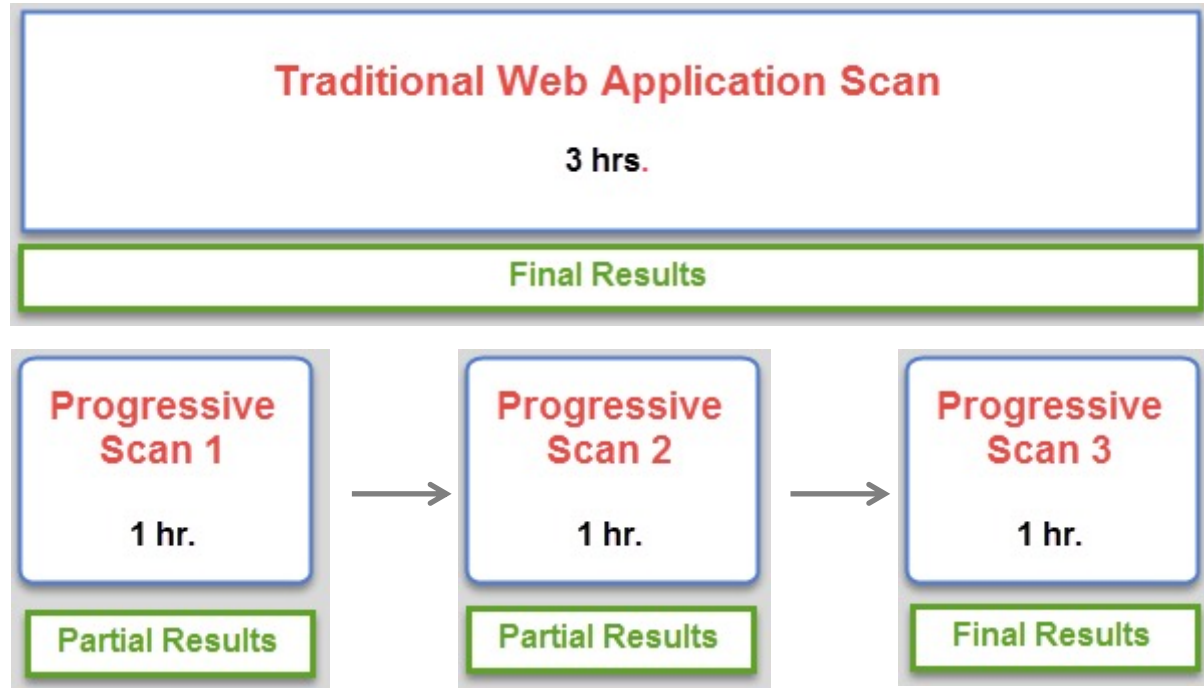
Burp Log File

You have the option to upload a Burp Log File with your scan tests. Once create requests and then crawl and test those requests.

[+ Upload Burp Log File](#)

Non-linked URLs or Web Services
(must be consistent with selected scope)

Web Application - Progressive Scanning



Works best with Frequently Scheduled Scans

Web Application - Progressive Scanning

- Performs 'look back' at previous scans
- Prioritizes pages not previously crawled
- Prioritizes new functionality
- Includes vulnerable pages detected previously
- Enhances flexibility in scheduling

Web Application - Redundant Links

Specify fully customizable patterns of redundant links so that the scan may not spend time crawling the similar links.

Web Application Edit: My First App

Turn help tips: On | Off Launch help

Edit Mode

Asset Details

Application Details

Scan Settings

DNS Override

Crawl Settings

Redundant Links

Authentication

Crawl Exclusion Lists

Malware Monitoring

Comments

Specify redundant links in your web application

Redundant Links

(*) REQUIRED FIELD

Specify links in the web applications for which contents are the same and because of which scan may spend too much time crawling and assessing these URLs. Links shall be specified as regular expressions so that you can specify an expression to match a list of links.

http://www.myshop.com/products/prod_[1-10].html

Check [guide](#) on how to format your regular expressions.

Specify the number of instances to be tested for each link identified by above regular expressions.

Max. Links to Crawl*

Web Application - Authentication

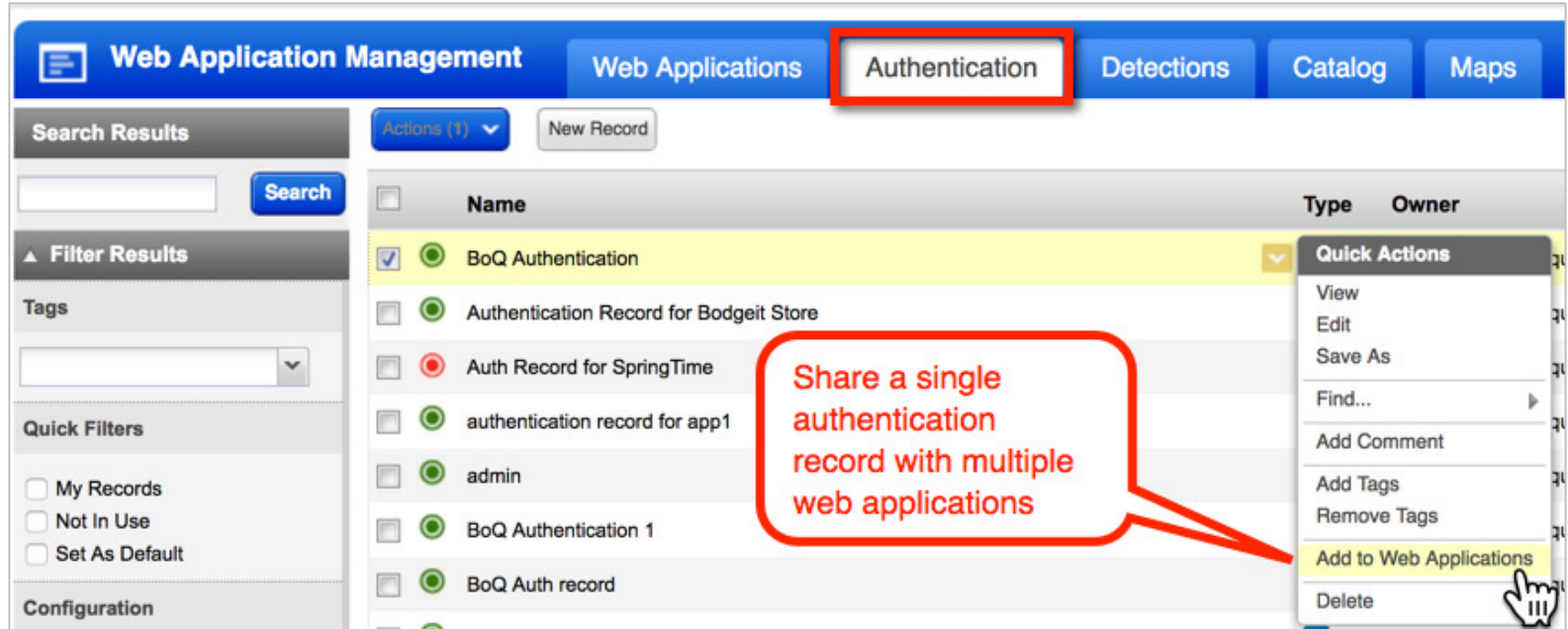
Form Records

- Standard Login
- Custom
- Selenium Script / Qualys Browser Recorder

Server Records

- Basic
- Digest
- NTLM

Manage Authentication Records



The screenshot displays the 'Web Application Management' interface. The top navigation bar includes tabs for 'Web Applications', 'Authentication' (highlighted with a red box), 'Detections', 'Catalog', and 'Maps'. Below the navigation bar, the 'Search Results' section shows a search bar and a 'Search' button. The 'Filter Results' section includes a 'Tags' dropdown and 'Quick Filters' with checkboxes for 'My Records', 'Not In Use', and 'Set As Default'. The main content area displays a table of authentication records. The first record, 'BoQ Authentication', is highlighted in yellow. A red callout box points to this record with the text 'Share a single authentication record with multiple web applications'. A 'Quick Actions' menu is open for the selected record, showing options like 'View', 'Edit', 'Save As', 'Find...', 'Add Comment', 'Add Tags', 'Remove Tags', 'Add to Web Applications' (highlighted), and 'Delete'. A hand cursor is pointing at the 'Add to Web Applications' option.

Name	Type	Owner
<input checked="" type="checkbox"/> BoQ Authentication		
<input type="checkbox"/> Authentication Record for Bodgeit Store		
<input type="checkbox"/> Auth Record for SpringTime		
<input type="checkbox"/> authentication record for app1		
<input type="checkbox"/> admin		
<input type="checkbox"/> BoQ Authentication 1		
<input type="checkbox"/> BoQ Auth record		

The Authentication tab provides a convenient place for managing both Form and Server authentication records.

Exclusions

White list

- Crawl specific directories or pages (within application scope).
- Content outside of 'white-list' is black-listed by default.
- Target a specific area of modified/updated code.

Black list

- Prevent WAS from crawling sensitive or protected locations.

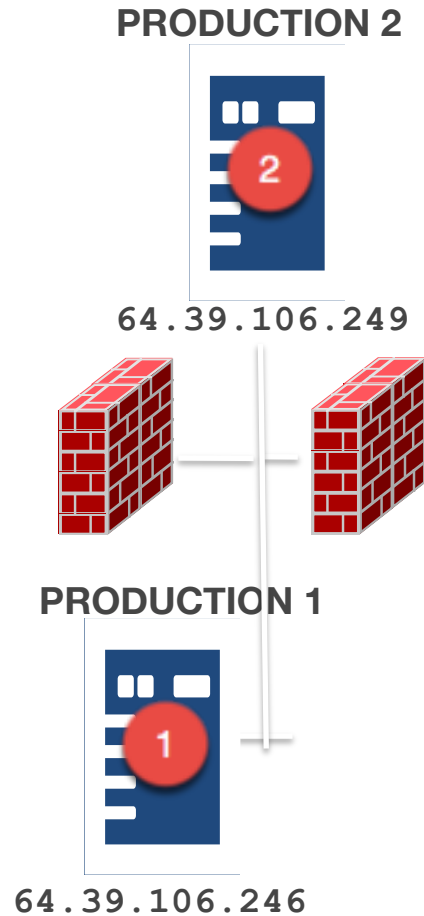
Post Data Black List

- Prevent WAS from posting HTTP forms on sensitive pages (i.e., Contact Us page).

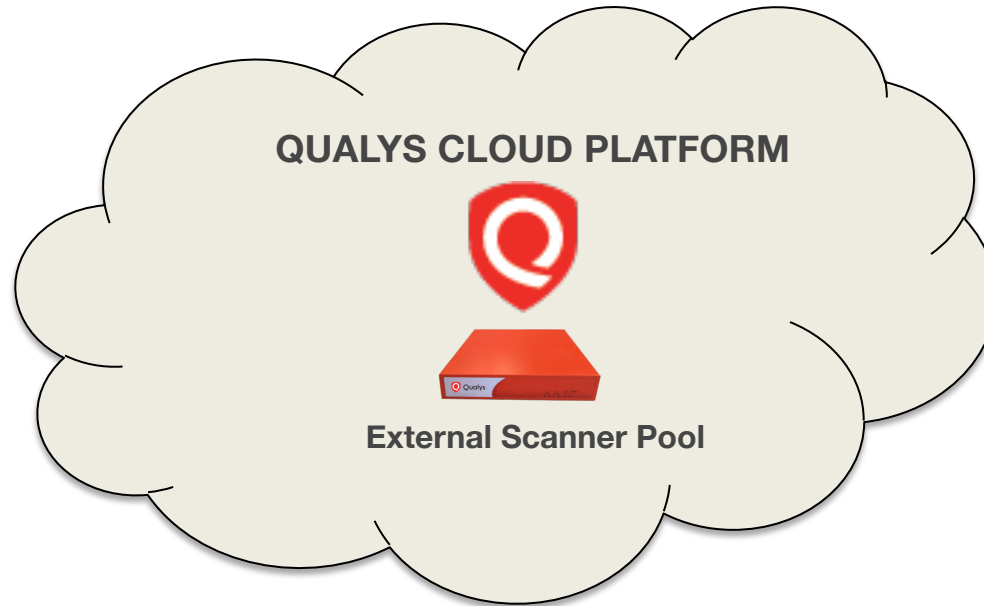
Logout Regular Expression

- WAS scanner will not crawl to specified 'logout' links.

Advanced Options - DNS Override



`www.yourwebapp.com:` 64.39.106.249



DNS Override Settings

DNS Override:

- Configure if DNS not yet configured for your app that's currently in Dev or QA
- Tag to manage assignment of DNS Override

New DNS Override Settings

Turn help tips: On | Off Launch help

Step 2 of 3

1 Basic Information

2 Mappings

3 Comments

Tell us the DNS settings you'd like to use

DNS Mappings (*) REQUIRED FIELDS

Define the mappings you prefer to use for scanning.

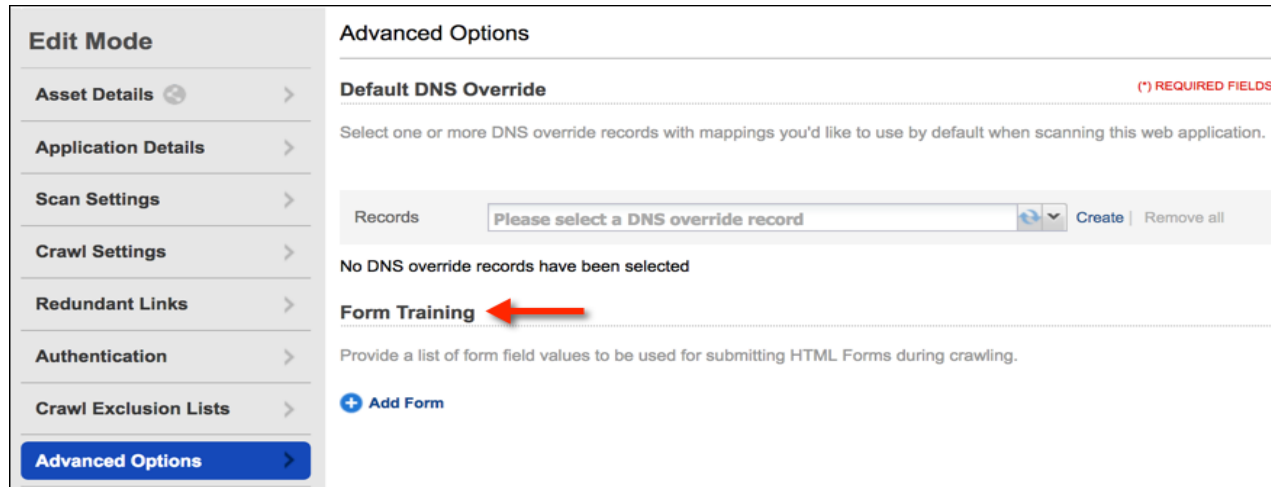
Host	IP Address	
example: my.host.com	example: 10.10.10.10	+ Add another
example.org	10.0.0.15	Remove

Cancel

PreviousContinue


Web Application - Form Training

- This is a way for us to tell WAS what data to submit in a form, to follow a certain workflow.
- Similar to how Qualys Recorder works. Works with just about any browser.



The image shows a web application interface with a sidebar on the left and a main content area on the right.

Sidebar (Edit Mode):



- Asset Details  >
- Application Details >
- Scan Settings >
- Crawl Settings >
- Redundant Links >
- Authentication >
- Crawl Exclusion Lists >
- Advanced Options >**

Main Content Area (Advanced Options):


Advanced Options

Default DNS Override (*) REQUIRED FIELDS

Select one or more DNS override records with mappings you'd like to use by default when scanning this web application.

Records   [Create](#) | [Remove all](#)

No DNS override records have been selected

Form Training 

Provide a list of form field values to be used for submitting HTML Forms during crawling.

[+ Add Form](#)

Web Application - Path Fuzzing

Use case: For testing sites that use URL re-writing (asp.net MVC)

Example: Let us consider sports web page

`http://www.abc.com/issue/17/section/sports/article/28`

However, the web server will read this URL as

`http://www.abc.com/search.php?issue=17§ion=sports&article=28`

The path fuzzing rule would be:

`http://www.abc.com/issue/{issue}/section/{section}/article/{article}`

No Web Service

The scan will give “No Web Service” status if the scanner:

- Cannot get a DNS lookup on the site
- Cannot reach the target because of routing
- Cannot get a web service to respond to a GET request

API Testing

APIs

- Provide a way for machine-to-machine communication
- Popular ones includes:
 - Representational State Transfer (REST) APIs
 - Simple Object Access Protocol (SOAP) APIs
- APIs use HTTP and are vulnerable to many of the same attacks as web applications

Qualys Support for SOAP APIs

- Supports basic security testing of SOAP based web services that have a Web Service Description Language (WSDL) file within the scope of the scan
- WAS uses the WSDL file to identify the web service methods and parameters supported
- WAS will attempt to perform XSS and SQL injection of the web services

Qualys Support for REST APIs

- RESTful web services can be exposed using files such as WADL (Web application description language), Swagger, or using proxy capture of the REST API client
- Qualys WAS captures the REST requests via an uploaded proxy capture of the REST API client
- Once the endpoints have been discovered, they can be tested for vulnerabilities

Qualys Support for openAPI (REST)

- Qualys WAS supports Swagger version 2.0 in JSON format
- If the Swagger file is available and successfully parsed, the APIs will be automatically tested for security flaws

Qualys Support for openAPI (REST)

Web Application CreationTurn help tips: On | Off Launch help

Step 1 of 11

1 Asset Details

2 Application Details

3 Scan Settings

4 Crawl Settings

5 Redundant Links

6 Authentication

Tell us about the asset you want to scan

Definition

Let's start with some basic information.

Name*

Example Website

Target Definition

Web Application URL (or Swagger file URL)*

https://

www.example.com/swagger.json

For scanning Swagger-based REST APIs, the Web Application URL should point to the Swagger file. It is your responsibility to verify that you have permission to scan all web applications or APIs that you specify as scan targets.

Lab 6, 7, 8 and 9

Please follow **pages 15 – 21** from the Lab Tutorial Supplement

Lab Supplement - <https://bit.ly/qsc2021-was>

Lab 6 – Sitemap

Lab 7 – Option Profile

Lab 8 – QBR Script 1

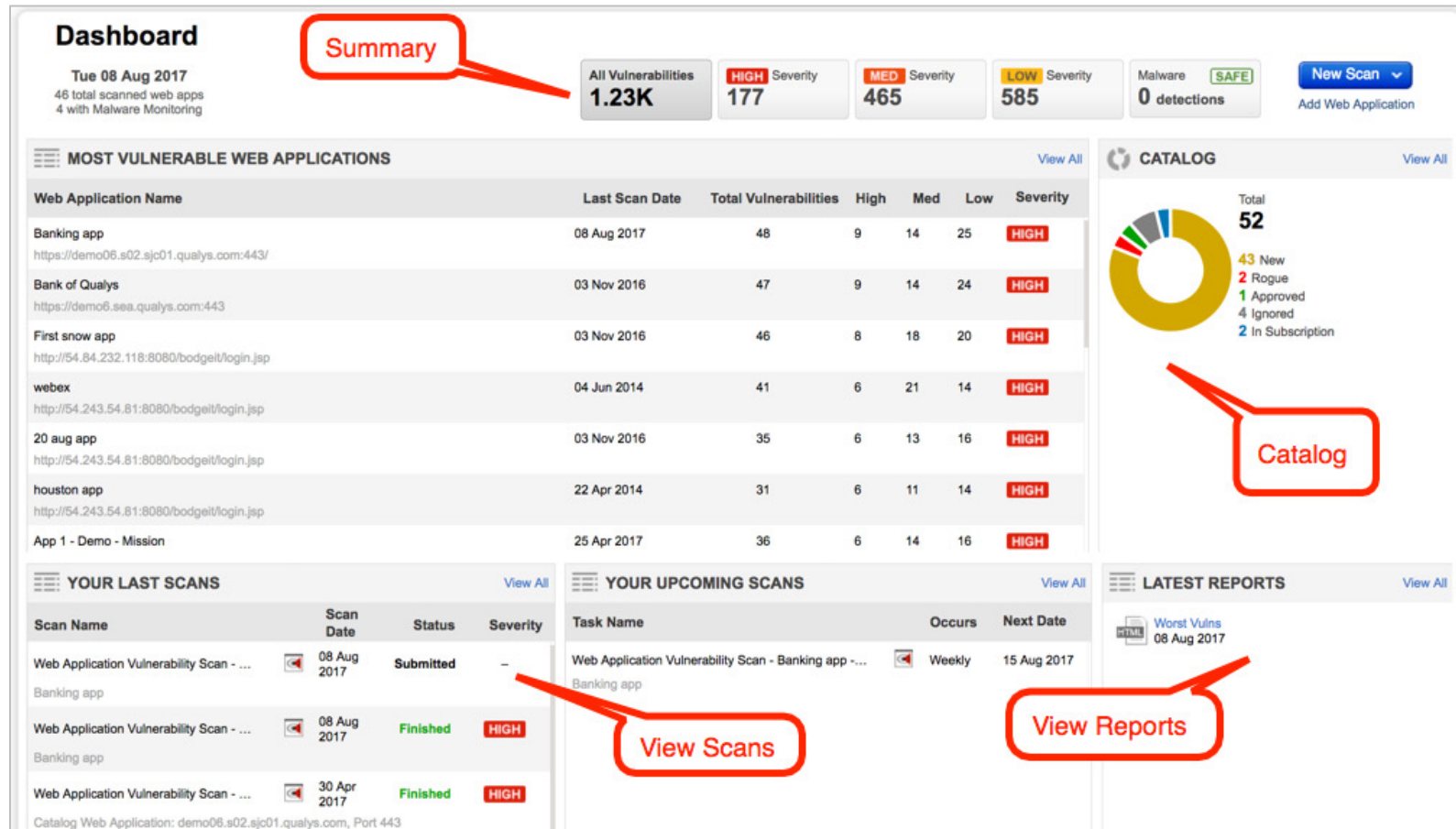
Lab 9 – QBR Script 2



25 min.

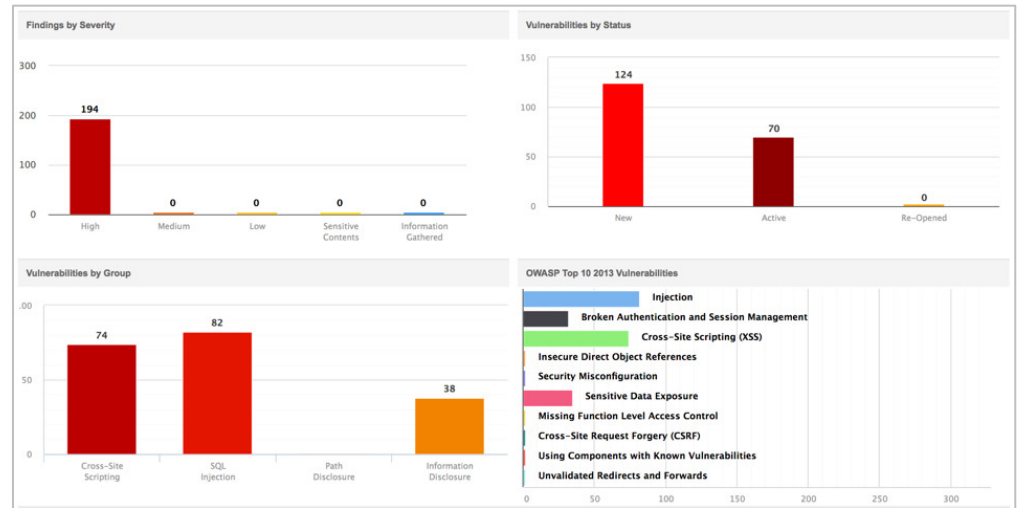
Reporting

Dashboard



WAS Reporting

- Results listed by vulnerability, link, type, app
- Redundant results are condensed to a base cause
- Create Templates to save report formats
- Four report types
- Schedule Reports to run when you need them



Web Application Report

- Normalized data of all scans on the web application
- Choose tags or applications for report targets
- Vulnerability Status included (New, Active, Re-opened, Fixed)
- History of vulnerability
- Retest for vulnerability

The screenshot displays a 'Vulnerability Details' window for a high-severity issue. Red callouts highlight the following elements:

- Retest, ignore, patch**: A button group at the top right of the vulnerability entry.
- Status**: A label pointing to the 'Active' status indicator.
- Vulnerable parameter**: A label pointing to the 'Parameter' field in the detection information section.
- History**: A label pointing to the 'View History...' link.
- Payload, Request, Response**: A label pointing to the request details in the '#1 Request' section.

Vulnerability Details

HIGH 150013 Browser-Specific Cross-Site Scripting Vulnerab
URL: http://54.84.232.118:8080/bodgeit/search.jsp

Retest, ignore, patch Install Patch Ignore Retest **Active**

Finding #	2870757	Web Application	10 Sept - Webex
Patch #	-	Authentication	Not Used
Group	Cross-Site Scripting		
CWE	CWE-79	First Time Detected	03 Nov 2016 11:55AM GMT-0500
OWASP	A3 Cross-Site Scripting (XSS)	Last Time Detected	03 Nov 2016 11:55AM GMT-0500
WASC	WASC-8 Cross-Site Scripting	Last Time Tested	03 Nov 2016 11:55AM GMT-0500
CVSS Base	4.3	Times Detected	3 View History...
CVSS Temporal	4.3		

Details Vulnerable parameter History Show

Detection Information

Parameter: It has been detected by exploiting the parameter **q** of the form located in URL **http://54.84.232.118:8080/bodgeit/search.jsp**

Access Path: The payloads section will display a list of tests that show how the param could have been exploited to collect the information
Here is the path followed by the scanner to reach the exploitable URL:

http://54.84.232.118:8080/bodgeit/login.jsp

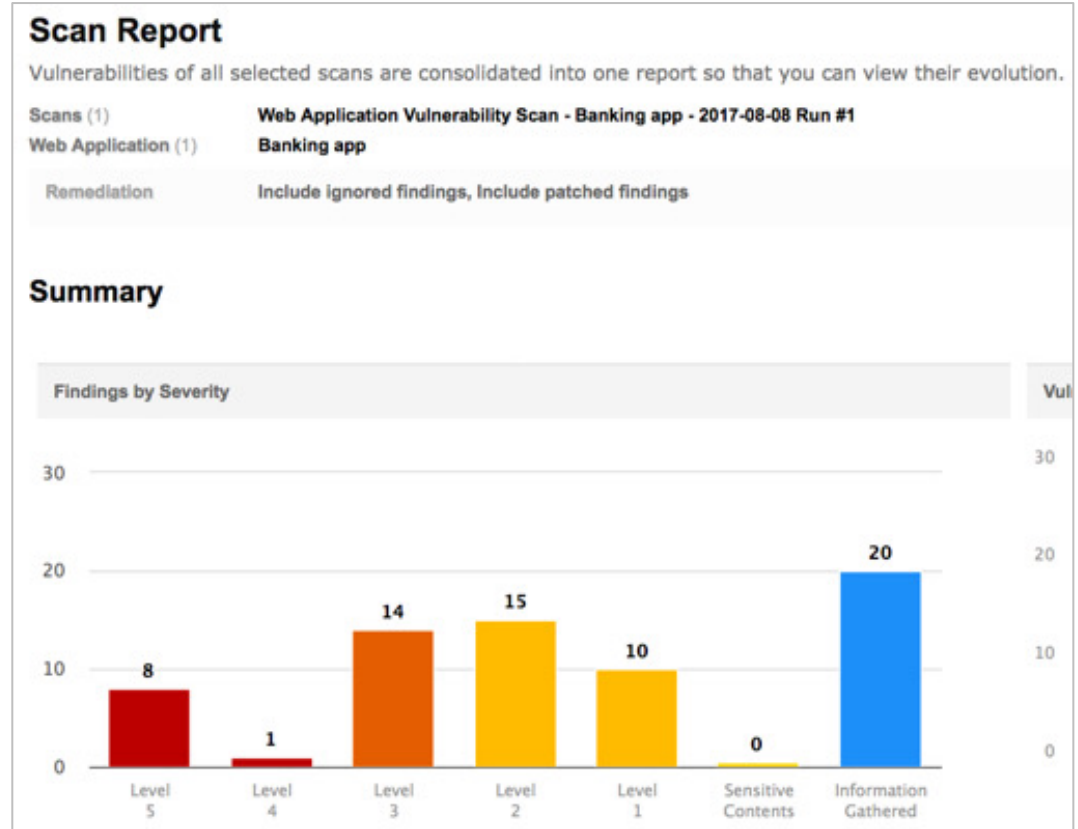
Payloads

#1 Request Show headers...

Payload: q=%3Cscript%20src%3Dhttp%3A%2F%2Flocalhost%2Fj%20
Request: GET http://54.84.232.118:8080/bodgeit/search.jsp?q=%3Cscript%20src%3Dhttp%3A%2F%2Flocalhost%2Fj%20

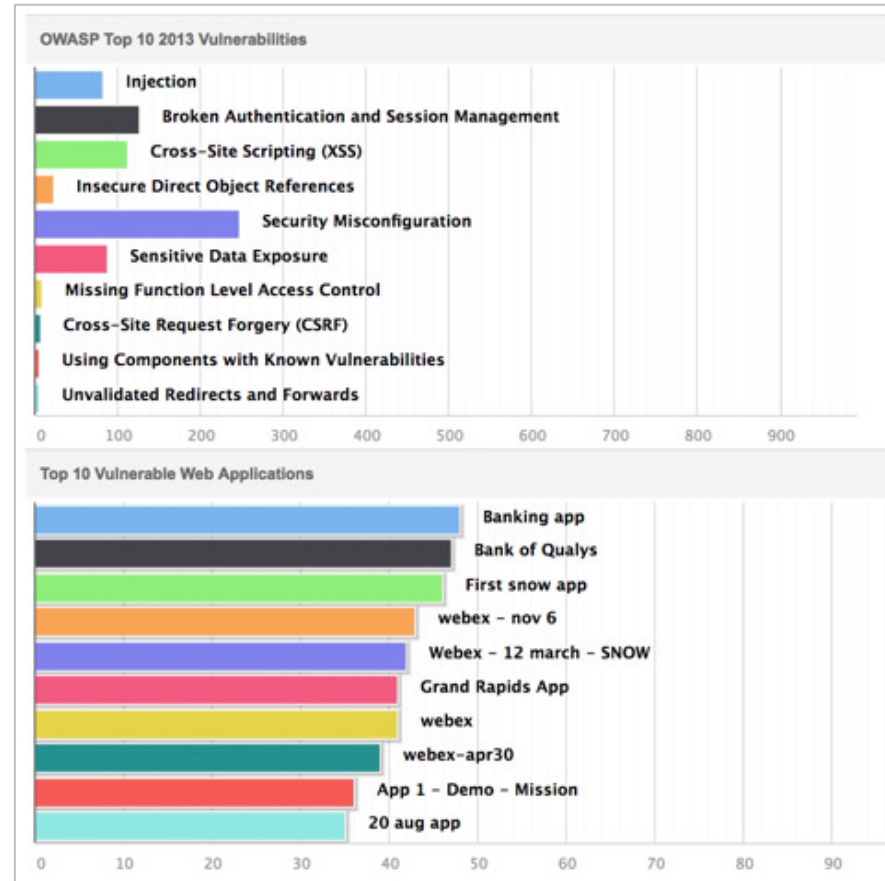
Scan Report

- Raw Scan Results
- Pick the specific scan results you'd like to view in a report
- View Threat, Impact, and Solution for vulnerabilities



Scorecard Report

- Statistics on all applications tagged in UI
- Top 10 most vulnerable applications
- OWASP breakdowns



Catalog Report

- Lists web apps as New, Approved, Rogue, or Ignored
- Number of entries added over time
- Number of entries by status



Report Management

- Create, download, run reports
- Filter existing reports
- Add tags to reports

The screenshot displays the 'Report Management' interface. At the top, there are tabs for 'Reports', 'Schedules', and 'Templates'. Below the tabs, there's a 'Search Results' section with a search bar and a 'Search' button. To the right of the search bar, there's an 'Actions (1)' dropdown and a 'New Report' button. Below the search bar, there's a 'Filter Results' section with a 'Tags' dropdown and a 'Quick Filters' section. The 'Quick Filters' section includes checkboxes for 'My Reports', 'Type', 'Format', 'Status', 'Generation Date', and 'Last Download Date'. A red callout box points to the 'Quick Filters' section with the text: 'Filter by tag, type, format, status, generation date, download date'. Below the filters, there's a 'Preview' section for the 'Worst Vulns' report. The preview shows the report type as 'Web Application Report', generated by 'MANAGER Nick (quays2nd2)' on '08 Aug 2017'. It also shows the format as 'Web Archive (HTML)', the template as 'Worst Vulns', and the tags as '-'. The 'Worst Vulns' report is highlighted in yellow in the main list.

Report Management Reports Schedules Templates

Search Results

Search

Filter Results

Tags

Quick Filters

☐ My Reports

Type

☐ Web Application Report
☐ Scan Report
☐ Scorecard Report
☐ Catalog Report
☐ Datalist Report

Format

☐ HTML (Zipped)
☐ Web Archive (HTML)
☐ PDF Document
☐ PDF (Encrypted)
☐ Word Document
☐ PowerPoint
☐ XML
☐ CSV

Status

☐ Complete ☐ Running
☐ Error

Generation Date

Select a date

Last Download Date

Select a date

Preview

Worst Vulns

Type: Web Application Report
Generated by MANAGER Nick (quays2nd2) | 08 Aug 2017

Format: Web Archive (HTML)
Template: Worst Vulns
Tags: -

QID 150021 – Scan Diagnostics

The scan diagnostics data provides technical details about the crawler's performance and behavior.

150021 Scan Diagnostics

Finding #	963158* (229849934)	Web Application	My First App
Group	Information Gathered	Authentication	Not Used
CWE	-		
OWASP	-	Detection Date	14 Feb 2017 12:54PM GMT
WASC	-		

Details Show


Results

☒ Highlight changes from previous scan

New - this link was not found in the previous scan

Modified - this result was found by the previous scan but its value was different

Removed - this link was not found, but was reported in the previous scan

 Export...

First column indicates HTTP response code,

Path manipulation: Estimated requests (payloads x links): files with extension:(4 x 27) + files:(15 x 27) + directories:(88 x 3) + paths:(15 x 30) = total (1227)

Batch #0 WS Directory Path manipulation: estimated time < 1 minute (9 tests, 30 inputs)

WS Directory Path manipulation: 9 vulnsigs tests, completed 27 requests, 1 seconds. Completed 27 requests of 27 estimated requests (100%). All tests completed.

Batch #0 WS enumeration: estimated time < 10 minutes (10 tests, 30 inputs)

WS enumeration: 10 vulnsigs tests, completed 30 requests, 0 seconds. Completed 30 requests of 300 estimated requests (10%). All tests completed.

Batch #1 URI parameter manipulation (no auth): 48 vulnsigs tests, completed 47 requests, 2 seconds. Completed 47 requests of 48 estimated requests (97.9167%). All tests completed.

Batch #1 Form parameter manipulation (no auth): 48 vulnsigs tests, completed 658 requests, 24 seconds. Completed 658 requests of 720 estimated requests (91.3889%). All tests completed.

Batch #1 URI blind SQL manipulation (no auth): 9 vulnsigs tests, completed 18 requests, 1 seconds. Completed 18

QID 150100 – Selenium Diagnostics

Troubleshoot
Selenium script

See which parts of
the script ran

150100 Selenium Diagnostics

Finding #	1190291* (248241167)	Web Application	My First App
Group	Information Gathered	Authentication	Not Used
CWE	-		
OWASP	-	Detection Date	04 Oct 2017 1:47PM GMT+0100
WASC	-		

Details

Results

☒ Highlight changes from previous scan

- New - this link was not found in the previous scan
- Modified - this result was found by the previous scan but its value was different
- Removed - this link was not found, but was reported in the previous scan

Log for Selenium script: crawlscrip
Executing: open | http://34.201.91.241:8080/bodgeit/basket.jsp | |
Executing: clickAndWait | link=Widgets | |
Executing: clickAndWait | link=Weird Widget | |
Executing: clickAndWait | id=submit | |

Lab 10 and 11

Please follow **page 22** from the Lab Tutorial Supplement

Lab Supplement - <https://bit.ly/qsc2021-was>

Lab 10 – Web App Report

Lab 11 – Scan Report



15 min.

Tags and Users

Tag Management

Add and remove tags to:

- Users
- Web Applications
- Reports
- Option Profiles
- Brute Force Lists
- Search Lists
- Scanners
- Parameter Sets
- Authentication Records



User Roles

- User roles provide privileges to access tagged assets
- Set granular permissions
- Grant QA or Developers access

The screenshot displays the 'User Edit' interface for a user named 'SCANNER Egon (quays2eb11)'. The interface is divided into a left sidebar and a main content area. The sidebar contains links for 'Edit Mode', 'User Details', 'Profile Settings', 'Roles And Scopes' (highlighted in blue), 'Action Log', and 'Account Activity'. The main content area is titled 'Edit role(s) and scope' and contains two sections: 'Edit role(s)' and 'Edit Scope'. In the 'Edit role(s)' section, there is a checkbox labeled 'Allow user full permissions and scope' which is checked and highlighted with a red box. Below this, there is a 'New role' button and a search bar for 'unassigned roles'. The 'Assigned roles' list shows 'WAS MANAGER' with a 'Remove' link. The 'Unassigned roles' list includes 'READER', 'UNIT MANAGER', 'WAF Manager', 'WAS SCANNER', and 'WAS USER', each with an 'Add' link. In the 'Edit Scope' section, there is a checkbox labeled 'Allow user view access to all objects' which is checked and highlighted with a red box. Below this, there is a 'Global Scope' section with a 'Select | Create | Remove All' link. The 'Global Scope' section shows three tags: 'Development', 'Production', and 'WebApps', each with a close button. A red callout box points to the 'WebApps' tag with the text 'Use tags on what the user should have access to'. At the bottom of the interface, there are 'Cancel' and 'Save' buttons.

User Edit: SCANNER Egon (quays2eb11) Turn help tips: On | Off

Edit Mode

- User Details
- Profile Settings
- Roles And Scopes**
- Action Log
- Account Activity

Edit role(s) and scope

☒ **Allow user full permissions and scope** (The user will have full access to everything)

Each role grants you a set of permissions that will apply to the objects you have access to.

New role

Assigned roles Remove all

- WAS MANAGER Remove

Unassigned roles Add all

- READER Add
- UNIT MANAGER Add
- WAF Manager Add
- WAS SCANNER Add
- WAS USER Add

Edit Scope

☒ **Allow user view access to all objects** (Other permissions are granted by the user's roles)

Define what assets the user can access by tags.

Global Scope Select | Create | Remove All

Development Production WebApps

User roles

Use tags on what the user should have access to

Cancel Save

Customize a role

WAS

Web Application Scanning

[Remove](#)

▶ **WAS Asset Permissions (8 of 8)**

▶ **Scanner Appliance Permissions (1 of 1)**

▼ **WAS Scan Permissions (3 of 3)**

☒ Launch WAS Scan

☒ Cancel WAS Scan

☒ Delete WAS Scan

▶ **WAS Schedule Permissions (3 of 3)**

▶ **WAS Configuration Permissions (22 of 22)**

▶ **WAS Catalog Permissions (4 of 4)**

▶ **WAS Burp Permissions (7 of 7)**

▶ **WAS Remediation Permissions (3 of 3)**

▶ **WAS Authentication Record Permissions (3 of 3)**

Lab 12 and 13

Please follow **pages 23 – 26** from the Lab Tutorial Supplement

Lab Supplement - <https://bit.ly/qsc21-was>

Direct Links:

- Lab 12 – Tagging
- Lab 13 – Users

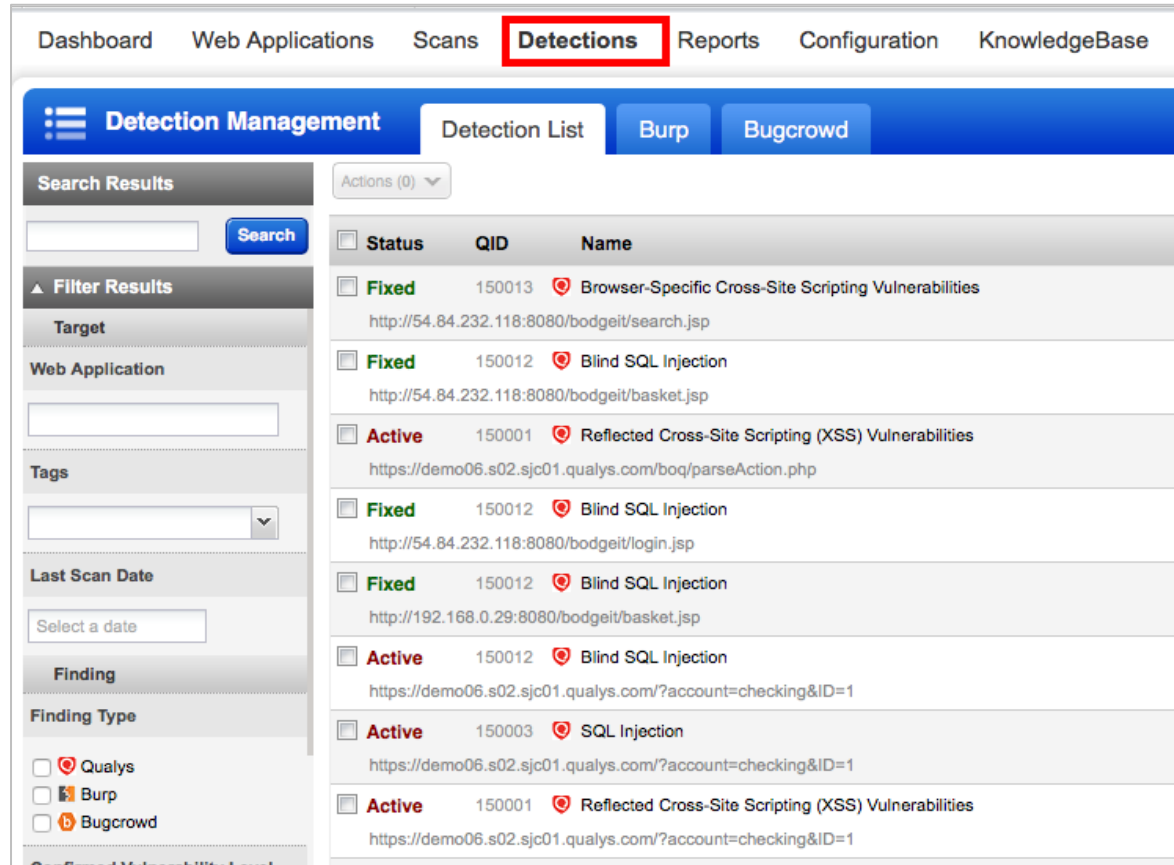


15 min.

Burp and Bugcrowd Integration

WAS Integration

- Centralized location for vulnerability details.



The screenshot displays the 'Detections' page in the WAS Integration interface. The top navigation bar includes 'Dashboard', 'Web Applications', 'Scans', 'Detections' (highlighted with a red box), 'Reports', 'Configuration', and 'KnowledgeBase'. Below this, the 'Detection Management' section is active, with tabs for 'Detection List', 'Burp', and 'Bugcrowd'. The left sidebar contains filters for 'Search Results', 'Filter Results', 'Target', 'Web Application', 'Tags', 'Last Scan Date', 'Finding', and 'Finding Type'. The main content area shows a table of detected vulnerabilities.

Status	QID	Name
Fixed	150013	Browser-Specific Cross-Site Scripting Vulnerabilities http://54.84.232.118:8080/bodgeit/search.jsp
Fixed	150012	Blind SQL Injection http://54.84.232.118:8080/bodgeit/basket.jsp
Active	150001	Reflected Cross-Site Scripting (XSS) Vulnerabilities https://demo06.s02.sjc01.qualys.com/boq/parseAction.php
Fixed	150012	Blind SQL Injection http://54.84.232.118:8080/bodgeit/login.jsp
Fixed	150012	Blind SQL Injection http://192.168.0.29:8080/bodgeit/basket.jsp
Active	150012	Blind SQL Injection https://demo06.s02.sjc01.qualys.com/?account=checking&ID=1
Active	150003	SQL Injection https://demo06.s02.sjc01.qualys.com/?account=checking&ID=1
Active	150001	Reflected Cross-Site Scripting (XSS) Vulnerabilities https://demo06.s02.sjc01.qualys.com/?account=checking&ID=1

Burp Suite Professional Integration

The screenshot displays the Burp Suite Professional interface. The top menu bar includes 'Burp', 'Intruder', 'Repeater', 'Window', and 'Help'. Below this is a toolbar with buttons for 'Target', 'Proxy', 'Spider', 'Scanner', 'Intruder', 'Repeater', 'Sequencer', 'Decoder', 'Comparer', 'Extender', 'Options', and 'Alerts'. The main window has a tabbed interface with 'Site map' and 'Scans' visible. The 'Scans' tab is active, showing a 'Dashboard' with 'Web Applications', 'Scans', 'Detections', 'Reports', 'Configuration', and 'KnowledgeBase'.

The 'Detections' tab is selected, showing a 'Detection List' with 'Burp' and 'Bugcrowd' filters. The 'Search Results' section on the left includes a search bar, a 'Search' button, and a 'Filter Results' section with 'Clear All' and 'Target' filters. The 'Web Application' filter is set to 'http://34.201.91.241:8080/bodgeit/contact.jsp'. The 'Tags' filter is set to 'New'. The 'Last Scan Date' is 'Select a date'. The 'Finding Type' section shows 'Qualys' and 'Burp' selected, with 'Bugcrowd' unselected.

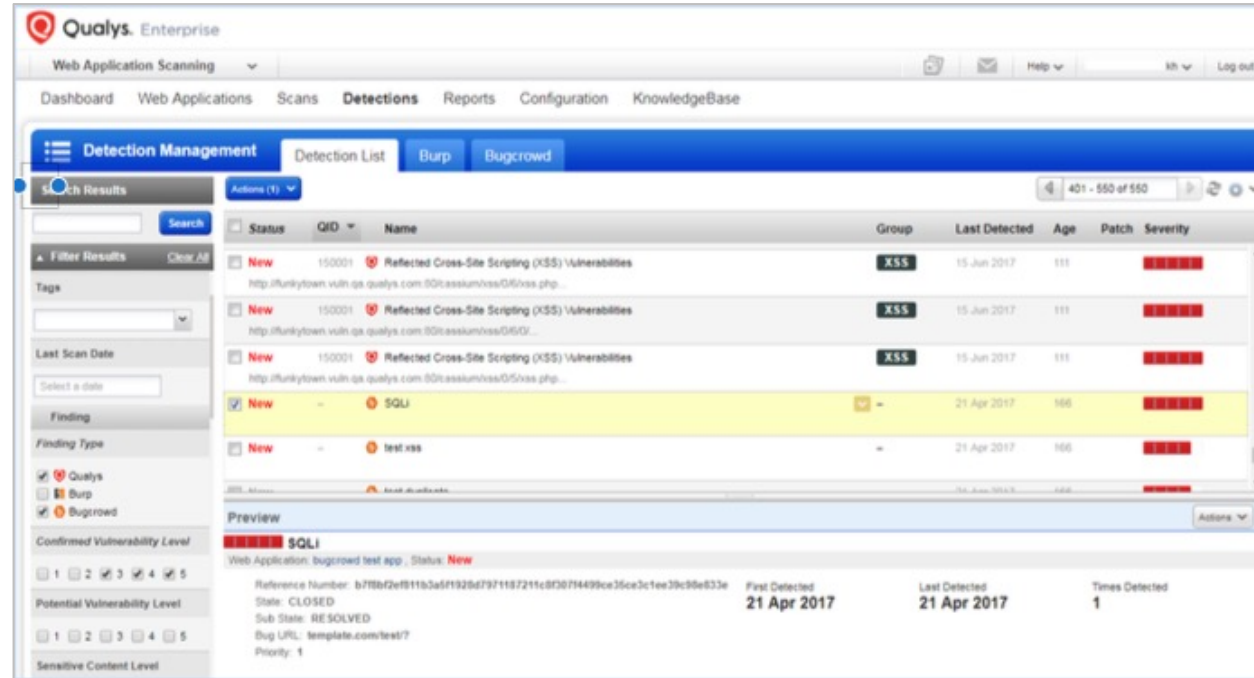
The main table displays the following data:

Status	QID	Name	Group	Last Detected	Age	Patch	Severity
Active	—	Password field with autocomplete enabled	—	15 May 2013	1635	—	High
—	—	HTML does not specify charset	—	15 May 2013	1635	—	Medium
—	—	HTML does not specify charset	—	15 May 2013	1635	—	Medium
New	—	Cleartext submission of password	—	15 May 2013	1635	—	Critical
New	—	Cookie without HttpOnly flag set	—	15 May 2013	1635	—	High
—	—	Frameable response (potential Clickjacking)	—	15 May 2013	1635	—	Medium
—	—	HTML does not specify charset	—	15 May 2013	1635	—	Medium
—	—	HTML does not specify charset	—	15 May 2013	1635	—	Medium

The bottom of the interface shows a search bar with the text 'Type a search term' and a '0 matches' indicator.

Bugcrowd Integration

- Qualys WAS and Bugcrowd can now bi-directionally import and export findings



Qualys Enterprise

Web Application Scanning

Dashboard Web Applications Scans **Detections** Reports Configuration KnowledgeBase

Detection Management Detection List Burp Bugcrowd

Search Results Search

Filter Results Clear All

Tags

Last Scan Date

Finding

Finding Type

Confirmed Vulnerability Level

Potential Vulnerability Level

Sensitive Content Level

Status	QID	Name	Group	Last Detected	Age	Patch	Severity
New	150001	Reflected Cross-Site Scripting (XSS) Vulnerabilities	XSS	15 Jun 2017	111		High
New	150001	Reflected Cross-Site Scripting (XSS) Vulnerabilities	XSS	15 Jun 2017	111		High
New	150001	Reflected Cross-Site Scripting (XSS) Vulnerabilities	XSS	15 Jun 2017	111		High
New	-	SQLi	-	21 Apr 2017	166		High
New	-	test.xss	-	21 Apr 2017	166		High

Preview

SQLi

Web Application: bugcrowd test app, Status: New

Reference Number: b7fbbf2efb1b3af5f1325d7971187211c8f3d714499ce35ce3c1ee39c95e633e

State: CLOSED

Sub State: RESOLVED

Bug URL: template.com/test/?

Priority: 1

First Detected: 21 Apr 2017

Last Detected: 21 Apr 2017

Times Detected: 1

Web Malware Detection

Malware Detection

You plug in your URL



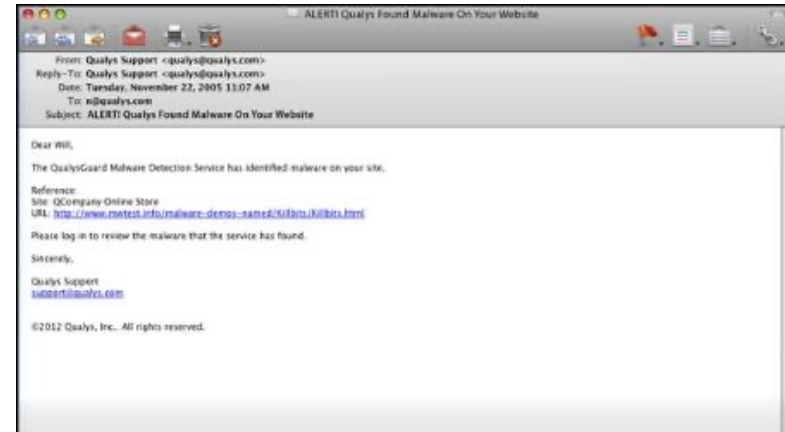
Malware Detection Service



Qualys Virtual
Machine Farm



1. Enter URL
2. MDS does a breadth crawl URL (we stay in the domain).
3. MDS runs both behavioral and static analysis.
4. Qualys will email user if Malware is found.



Malware Detection

Web Application Scanning Help MANAGER

Dashboard Web Applications Scans Burp Reports Configuration KnowledgeBase

Dashboard

Fri 26 Sep 2014
24 total scanned web apps
0 with Malware Monitoring

All Vulnerabilities 645	HIGH Severity 94	MED Severity 243	LOW Severity 308	Malware SAFE 0 detections
-----------------------------------	-----------------------------------	-----------------------------------	-----------------------------------	--

Dashboard Web Applications Scans Burp Reports Configuration KnowledgeBase

Web Application Management

Web Applications Detections Catalog Maps

Search Results Search

Filter Results

Tags

Actions New Web Application Import New Scan New Schedule 1 - 1 of 1

<input type="checkbox"/>	Name	# Pages	# Vulns	Severity	MDS Severity	Updated
<input type="checkbox"/>	My First app http://54.243.54.81:8080/bodgeit/login.jsp	30	19	HIGH	SAFE	15 May 2013

Lab 14

Please follow **page 27** from the Lab Tutorial Supplement

Lab Supplement - <https://bit.ly/qsc2021-was>

Lab 14 – Burp Integration



5 min.

Course Survey





Qualys®

Thank You

training@qualys.com